VOTE EXPLANATION

Mr. BIDEN. Madam President, I was unable to be here for an earlier vote today. I was at the funeral of a brave young American, Aerographer's Mate Second Class Matthew Michael Flocco, whose life was one of those so tragically ended at the Pentagon on September 11. I believed it was important to be there with the family, to make sure they knew that America shares in their grief and stands ready to assist them in any way we can.

CRITICAL INFRASTRUCTURE INFORMATION SECURITY ACT

Mr. BENNETT. Madam President, yesterday Senator KYL and I introduced the Critical Infrastructure Information Security Act, CIISA, which is designed to minimize a dangerous national security blind spot by: one, protecting voluntarily shared critical infrastructure information; two, providing critical infrastructure threat analysis; and three, encouraging proactive industry cooperation.

Critical infrastructures are those key sectors such as financial services, telecommunications, transportation, energy, emergency services, and government essential services, whose disruption or destruction would impact our economic or national security. On September 11, 2001, America suffered a senseless strike, where America's commercial air space was ''weaponized'' and turned viciously against its financial and defense establishments in an infrastructure attack that resulted in staggering losses.

About 85 percent of the United States' critical infrastructures, telecommunications, energy, finance, and transportation systems, are owned and operated by private companies. If our critical infrastructures are targets, it is the private sector that is on the front line. Thus, we have to think differently about national security, as well as who is responsible for it. In the past, the defense of the Nation was about geography and an effective military command-and-control structure. However, now prevention and protection must shift from the command-control structure to partnerships that span private and government interests.

The American economy is a highly interdependent system of systems, with physical and cyber components. Preventing, detecting, responding, mitigating, and recovering from attacks to these systems requires an unprecedented exchange of information. It is essential to remove unnecessary barriers that prevent the private sector from sharing information. Because in many cases, releasing sensitive information into the public domain could have extremely negative consequences for business, it is understandable why the private sector is reticent to share this information with the Government as it is not protected.

The Critical Infrastructure Information Security Act, CIISA, is intended to clear the way for increased critical infrastructure information sharing and improve threat analysis for these infrastructures. The bill seeks to increase the two-way sharing of information between the Federal Government and the private sector by first, protecting information voluntarily shared by the private sector, and second, requiring the Government to send analysis back to the private sector. It also encourages information sharing within the private sector so industry can better solve its own problems.

CIISA outlines a process by which critical infrastructure information, information which would not normally be shared due to its sensitivity, can be submitted to one of 13 designated Federal agencies with a request that the information be protected. Such a request would mean that this information will not be disclosed even in a response to a request under the Freedom of Information Act, commonly known as FOIA.

FOIA has helped make a transparent government. Initially enacted in 1966, FOIA establishes for any person, corporate or individual, regardless of nationality, presumptive access to existing, unpublished agency records on any topic. CIISA does not change FOIA in any way. In fact, it seeks to protect information which would not be in the public domain in the first place and if publicly released, could interfere with, disrupt, or compromise critical infrastructure operations. CIISA will protect voluntarily shared information without diminishing Federal transparency.

Access to information is essential to our democracy. However, it is important to realize that the ability to make a request under FOIA does not apply only to American citizens interested in seeing what the Government is doing. Corporations, associations, foreign citizens, and even foreign governments have the same access. There are no limitations on FOIA even during times of war. Furthermore, the narrow provisions provided in CIISA are nothing new. Congress has on 40 other occasions created certain classes of information that are not subject to the Freedom of Information Act.

In order to ensure the uniform protection of voluntarily shared information, CIISA requires the Director of the Office of Management and Budget to establish procedures for the Federal agencies to receive, acknowledge, mark, care, and store voluntarily submitted critical infrastructure information. Today, there is no uniform standard of care under FOIA.

CIISA requires that information and analyses from the Federal Government be shared back with the private sector in the form of notifications, warnings, and strategic analyses. The bill requires a Federal agency receiving voluntarily submitted critical infrastructure information to make reasonable efforts to do the following: one, analyze the information; two, determine the tactical and strategic implications for such information; three, identify interdependencies; and four, consider conducting further analysis in concert with other Federal agencies. Following this analysis, a Federal agency may issue warnings regarding potential threats to: one, individual companies; two, targeted industry sectors; three, the general public; or four, other government entities. Federal agencies must take appropriate actions to prevent the disclosure of the source of any voluntarily submitted critical infrastructure information that forms the basis for any warnings.

CIISA also requires the President to designate an entity within the executive branch to conduct strategic analyses of potential threats to critical infrastructure; and to submit reports and analyses to information sharing and analysis organizations and the private sector. These analyses draw upon this information submitted to the Federal Government by the private sector, as well as information from the Federal Government, such as national security and law enforcement information. The President is also required to submit a plan for developing strategic analysis capabilities in the Congress.

When competitors work closely to address common problems, antitrust concerns always surface. Security in a networked world must be a shared responsibility. To encourage the private sector to find solutions to common security problems, CIISA provides a narrow antitrust exemption, not unlike that of the Information Readiness Disclosure Act or the Defense Production Act. Information sharing and analysis organizations formed solely for the purpose of gathering and analyzing critical infrastructure information and to help prevent, detect, mitigate or recover from the effects of a problem relating to critical infrastructure, will be exempt from antitrust laws. Again, this exemption only applies to the activities specifically undertaken to address infrastructure problems. The antitrust exemption will not apply to conduct that involves or results in an agreement to boycott any person, to allocate a maker, or to fix prices or output.

The threats to our critical infrastructure are varied. Some of those threats are physical; some may come from cyberspace. From wherever they come, the private sector and Government each has different vantage points. It is my hope that this bill will help both entities work together to reduce the blind spot.

I thank Senator KYL for his interest and leadership on this issue.

COMMENDING THE TRUCKING INDUSTRY

Mr. BROWNBACK. Madam President, I rise to speak today in recognition of the noble truck drivers across the Nation. For the past 2 weeks, our truckers have been valiant in their service to